4. *Савчук В.В.* Иконический поворот / В.В. Савчук // Философские науки. – 2010. – № 5. – С. 134-139.

5. *Скабалланович М.* Толковый Типикон. Объяснительное изложение Типикона. С историческим введением / М. Скабалланович. – М.: Изд. Сретенского монастыря, 2004. – 678 с.

6. *Ушаков С.* Слово к люботщательному иконного писания / С. Ушаков // Мастера искусства об искусстве. – М., 1969. Т. 6. – С. 52-58.

7. *Чейф У. Л.* Значение и структура языка / пер. с англ. Изд. 3. – М.: Эдиториал УРСС, 2009. – 424 с.

М. Я. ТОВШТЕЙН
кандидат физико-математических наук, доцент
Набережночелнинский институт
Казанского (Приволжского) федерального университета,
Россия, Набережные Челны
mark_tovst@mail.ru

РИСУНОК КАК СТЕГОКОНТЕЙНЕР В КОМПЬЮТЕРНОЙ КОММУНИКАЦИИ

Аннотация. Стеганография наряду с криптографией представляет проблемную область, которая имеет дело, в частности, с защитой информации от несанкционированного доступа. Криптография позволяет людям обмениваться сообщениями по незащищённому каналу связи, а стеганография помогает спрятать секретное сообщение в объекте, посылаемом открыто, не вызывая подозрений. В статье рассказывается о компьютерной программе, позволяющей внедрять зашифрованный текст в цифровое изображение и извлекать его с последующим расшифровыванием.

Ключевые слова: стеганография, криптография, защита информации от несанкционированного доступа.

Позвольте сначала пояснить, что же в названии статьи обозначает слово *стегоконтейнер*. Стего – так кратко называют *стегосообщение*, которое прячут в другом сообщении – *стегоконтейнере*, или, кратко, – *контейнере*. Эти термины используются в *стеганографии* [4; 9; 2]: от греческих *steganos* – скрытый и *grapho* – пишу. Так называется наука и искусство передавать скрытные (секретные) сведения внутри других – открытых – контейнерах.

Простейший пример. Мы в детстве не раз всматривались в замысловатую картинку, пытаясь разгадать, где в ней среди хитросплетений веточек волшебных деревьев, цветочков и травы «спрятался» зайчик или ещё какой-

нибудь персонаж. Так вот: искомый зайчик – это стегосообщение, а картинка с изображением лесной чащи – стегоконтейнер.

Стеганография наряду с криптографией представляет проблемную область, которая имеет дело, в частности, с защитой информации от несанкционированного доступа. Однако криптография занимается проектированием секретных систем, используя тонкие математические и алгоритмические методы шифрования, которые позволяют корреспондентам (их традиционно именуют Алисой и Бобом) обмениваться сообщениями с большой степенью уверенности, что эти сообщения никакой злодей не перехватит, а если и перехватит, то не сможет их прочитать и/или вставить(заменить) в них нечто от себя [1]. Стеганография же позволяет Алисе скрыть сам факт того, что в пересылаемом Бобу объекте – *контейнере* (тексте, картине или музыкальном произведении) спрятано некое секретное сообщение (*стего*) [7]. Причём Алиса может ещё и подстраховаться, зашифровав своё сообщение перед внедрением его в контейнер, на случай, если хитроумный злодей всё-таки найдёт способ обнаружить закладку.

В наше время представляется очевидным тот факт, что огромную роль в жизни общества играет компьютерная коммуникация. Вошедшие в обыденную практику персональные компьютеры, интернет, мобильные и, что очень важно, компактные телефоны и планшеты остро ставят задачи по защите информации, передаваемой по телекоммуникационным каналам.

Поэтому понятен интерес студентов кафедры системного анализа и информатики НЧИ К(П)ФУ, сотрудником которой я имею честь быть, к изучению методов, обеспечивающих информационную безопасность. В отличие от студентов юридического факультета [10], «IT-ориентированные» студенты нашей кафедры с бо́льшим пониманием изучают не столько правовые, административно-организационные или инженерно-технические методы, сколько методы *программной* защиты данных. С усердием и энтузиазмом они превращают в компьютерные программы непростые, требующие знания математики, алгоритмы шифрования и расшифровывания сообщений симметричными и асимметричными ключами, использования электронно-цифровой подписи, создания дайджеста посланного сообщения [1].

Однако наиболее «продвинутым» студентам недостаточно тех сведений, которые они получают во время аудиторных занятий. Им хочется создать нечто большее, чем очередную лабораторную работу. И тогда я им советую заняться задачами стеганографии. Они сначала выполняют курсовую работу, знакомясь со специфическими форматами различных контейнеров (файлы, содержащие изображения, а также текстовые, аудио- и видео-файлы), а затем и дипломную (ВКР – выпускную квалификационную) работу, продукт, имеющий практическое применение.

К теме нашей конференции относится ВКР Морозова А.В. «Разработка программной реализации стеганографического метода с выбором контейнера

для защиты текстового сообщения с применением криптографии», поскольку контейнером в этой работе служит цифровое изображение (фото, картина, рисунок). Расскажем о ней подробнее.

Обычно при внедрении сообщения в цифровое изображение используют наименее значимые биты изображения (Least Significant Bit) – LSB [5]. Они могут быть заменены данными из текстового файла так, что посторонний независимый наблюдатель не обнаружит никакой потери в качестве изображения. В данной работе используется вместе с алгоритмом LSB так называемый алгоритм JPEG [3], настроенный на преобразование файла формата JPEG.

Кратко алгоритм JPEG, на котором основан метод, выглядит так:

1) преобразование цветового пространства;
2) субдискретизация;
3) соединение в блоки;
4) дискретное косинус-преобразование;
5) квантование;
6) сжатие без потерь;
7) добавление заголовков и запись в файл.

Теперь изложим этот алгоритм чуть подробнее, но без пояснения профессиональных терминов.

1. Преобразование цветового пространства. Цветное изображение преобразуется из RGB в представление светимость/цветность. Глаз чувствителен к малым изменениям яркости пикселей, но не цветности, поэтому из компонентов цветности можно удалить значительную долю информации для достижения высокого сжатия без заметного визуального ухудшения качества образа. Этот шаг не является обязательным, но он очень важен, так как остальная часть алгоритма будет независимо работать с каждым цветным компонентом. Без преобразования пространства цветов из компонентов RGB нельзя удалить существенную часть информации, что не позволяет сделать сильное сжатие.

2. Субдискретизация. Для более эффективного сжатия цветное изображение разбивается на крупные пиксели. Укрупнение пикселей либо вообще не делается (укрупнение 1hv1 или «4:4:4»), либо же делается или в соотношении 2:1 по горизонтали и вертикали (укрупнение 2h2v или «4:1:1») или в пропорциях 2:1 по горизонтали и 1:1 по вертикали (укрупнение 2h1v или «4:2:2»).

3. Соединение в блоки. Пиксели каждой цветной компоненты собираются в блоки 8x8, которые называются единицами данных. Если число строк или столбцов изображения не кратно 8, то самая нижняя строка и самый правый столбец повторяются нужное число раз.

4. Дискретное косинус-преобразование. К каждой единице данных применяется дискретное косинус-преобразование, в результате чего получаются блоки 8x8 частот единиц данных. Они содержат среднее значение пикселей

единиц данных и следующие поправки для высоких частот. Это позволяет представить данные в виде, позволяющем более эффективное сжатие.

5. Квантование. Каждая из 64 компонент частот единиц данных делится на специальное число, называемое коэффициентами квантования, которое округляется до целого. Здесь информация невосполнимо теряется. Но в нашем кодировщике этот шаг опускается для увеличения количества записываемой информации (т.е. все коэффициенты квантования равны единице, качество JPEG – 100 %).

6. Сжатие без потерь. Все 64 квантованных частотных коэффициента каждой единицы данных кодируются с помощью комбинации RLE и метода Хаффмана.

7. Добавление заголовков и запись в файл. На последнем шаге добавляется заголовок из использованных параметров JPEG и результат выводится в сжатый файл.

Далее описан алгоритм кодировщика (декодер делает всё то же самое, но в обратном порядке).

На входе: цветное изображение, скрываемые данные, пароль.

На выходе: изображение в формате JPEG со скрытыми данными.

1. Генерация ключей. Для работы кодировщика необходимы два ключа: стеганоключ и криптоключ. Берется хэш-сумма SHA-256 [6] введённого пользователем пароля. Первые 16 байт будем использовать для стеганоключа, вторые – для криптоключа [4].

2. Предварительная обработка текста. Повторно берется хэш-сумма криптоключа и получаются новые 32 байта, которые уже будут использоваться для шифрования данных. Данные шифруются с помощью алгоритма AES-256 [1].

3. Начинается кодирование изображения. Проводятся первые 4 шага ранее рассмотренного алгоритма JPEG.

4. Вместо 5-го шага (квантование) алгоритма JPEG происходит встраивание сообщения.

Стеганопуть. Стеганоключ представляется в двоичном виде, и каждому блоку ставится в соответствие соответствующий бит двоичной последовательности (по модулю). Если бит равен единице, блок используется для записи, если нулю – то отбрасывается.

Стеганокодер. Проводится стандартная процедура LSB для каждого блока 8x8: данные записываются в каждый элемент, значение которого больше единицы.

5. Продолжает выполнение алгоритма JPEG (сжатие без потерь и запись в файл).

Программа работает в двух режимах: встраивания и извлечения сообщения.

В режиме встраивания сообщения пользователь (Алиса) вводит: ноль – признак режима встраивания; путь до файла-контейнера; внедряемое сообщение; пароль (секретный ключ), который должен быть известен только Алисе и Бобу (пароль может содержать буквы, цифры и знаки препинания).

Если встраивание прошло успешно, программа выдаст ободряющую фразу, в противном случае выдаст сообщение об ошибке.

В режиме *извлечения* сообщения пользователь (Боб) вводит: единицу – признак режима извлечения; путь до файла-контейнера, из которого хочет достать секретное сообщение; пароль (секретный ключ), известный только Бобу и Алисе. В результате Боб увидит либо сообщение Алисы, либо сообщение об ошибке.

На рисунке 1а представлено изображение до встраивания в него сообщения (пустой контейнер), а на рисунке 1б изображение после встраивания фразы «Любое секретнейшее сообщение!» (заполненный контейнер). Как можно увидеть, различия между этими изображениями не видны человеческому глазу. Это один из важных критериев стеганографии, так как указывает на стойкость разработанного метода к пассивным атакам.

Рис. 1 (а и б). Пустой и заполненный контейнеры

Стегоконтейнер в виде компьютерной картинки поможет не только незаметно переслать шифротекст, но и выполнить много других функций. Например, скрытно хранить некоторые сведения, защитить авторское право, доказать подлинность документа, подтвердить достоверность переданного сообщения и другие [8]. Так что те студенты, которые знают стеганографические и криптографические методы защиты данных и умеют ими пользоваться, являются профессиональными специалистами, представляющими большую ценность для грамотного работодателя.

ЛИТЕРАТУРА

1. *Аграновский А.В.* Практическая криптография: алгоритмы и программирование / А.В.Аграновский, Р.А. Хади. – М.: СОЛОН-Пресс, 2009. – 256 с.
2. *Артёхин Б.В.* Стеганография / Б.В. Артёхин // Защита информации. Конфидент. – 1996. – №4. – С.47-50.
3. *Быков С.Ф.* Алгоритм сжатия JPEG с позиции компьютерной стеганографии / С.Ф. Быков // Защита информации. Конфидент. – 2000. – № 3. – С.
4. *Генне О.В.* Основные положения стеганографии / О.В. Генне. – URL: http://www.compdoc.ru/secur/protect/stegano/ (дата обращения: 15.09.2016).
5. *Грибунин В.Г.* Цифровая стеганография / В.Г. Грибунин, И.Н.Оков, И.В.Туринцев. – М.: Солон-Пресс, 2002. – 272 с.
6. *Оков И.Н.* Криптографические системы защиты информации / И.Н. Оков. – СПб.: ВУС, 2001. – 236 с.
7. *Осипян В.О.* Криптография в задачах и упражнениях / В.О. Осипян, К.В. Осипян. – М.: Гелиос АРВ, 2004. – 144 с.
8. Стеганография в XXI веке. Цели. Практическое применение. Актуальность. – URL: https://habrahabr.ru/post/253045/ (дата обращения: 21.09.2016).
9. *Текин В.* Текстовая стеганография / В. Текин. – URL: http://www.osp.ru/pcworld/2004/11/169154/ (дата обращения: 25.09.2016).
10. *Товштейн М.Я.* О защите информации – будущим защитникам закона / М.Я. Товштейн // Прикладная дискретная математика. – 2009. – Приложение №1. – С.111-112.

Г. Р. ХАЙДАРОВА
доктор философских наук, доцент
Военный учебно-научный центр
«Военно-морская академия имени Н.Г. Кузнецова»
Россия, Санкт-Петербург
khaidarova@rambler.ru

ВНУТРИ ИМИДЖЕВЫХ ВОЙН

Статья выполнена в рамках исследовательского проекта «Новый тип рациональности в эпоху медиального поворота» № 16-18-10162, поддержанного фондом РНФ

Аннотация. В статье рассматривается новый тип медийных войн, основанный на борьбе за воображаемое. Визуальный коммуникативный слой, играющий роль объекта манипуляции, оказывается в первую очередь втянут в этот тип войны. Возникающий новый тип медиарациональности, включаю-